

# Non-Interactive Statistically-Hiding Quantum Bit Commitment from Any Quantum One-Way Function

Takeshi Koshihara

Takanori Odaira

Graduate School of Science and Engineering, Saitama University

## Abstract

We provide a non-interactive quantum bit commitment scheme which has statistically-hiding and computationally-binding properties from any quantum one-way function. Our protocol is basically a parallel composition of the previous non-interactive quantum bit commitment schemes (based on quantum one-way permutations, due to Dumais, Mayers and Salvail (EUROCRYPT 2000)) with pairwise independent hash functions. To construct our non-interactive quantum bit commitment scheme from any quantum one-way function, we follow the procedure below: (i) from Dumais-Mayers-Salvail scheme to a weakly-hiding and 1-out-of-2 binding commitment (of a parallel variant); (ii) from the weakly-hiding and 1-out-of-2 binding commitment to a strongly-hiding and 1-out-of-2 binding commitment; (iii) from the strongly-hiding and 1-out-of-2 binding commitment to a normal statistically-hiding commitment. In the classical case, statistically-hiding bit commitment scheme (by Haitner, Nguyen, Ong, Reingold and Vadhan (SIAM J. Comput., Vol.39, 2009)) is also constructible from any one-way function. While the classical statistically-hiding bit commitment has large round complexity, our quantum scheme is non-interactive, which is advantageous over the classical schemes. A main technical contribution is to provide a quantum analogue of the new interactive hashing theorem, due to Haitner and Reingold (CCC 2007). Moreover, the parallel composition enables us to simplify the security analysis drastically.

**Keyword:** quantum bit commitment, quantum one-way function, non-interactive

## 1 Introduction

A bit commitment is a fundamental cryptographic protocol between two parties. The protocol consists of two phases: commit phase and reveal phase. In the commit phase, the sender, say Alice, has a bit  $b$  in her private space and she wants to commit  $b$  to the receiver, say Bob. They exchange messages and at the end of the commit phase Bob gets some information that represents  $b$ . In the reveal phase, Alice confides  $b$  to Bob by exchanging messages. At the end of the reveal phase, Bob judges whether the information gotten in the reveal phase really represents  $b$  or not. Basically, there are three requirements for secure bit commitment: the

correctness, the hiding property and the binding property. The correctness guarantees that if both parties are honest then, for any bit  $b \in \{0, 1\}$  Alice has, Bob accepts with certainty. The hiding property guarantees that (cheating) Bob cannot reveal the committed bit during the commit phase. The binding property guarantees that (cheating) Alice cannot commit her bit  $b$  such that Alice maliciously reveal  $b \oplus 1$  as her committed bit but Bob accepts.

In the classical case, a simple argument shows the impossibility of bit commitment with the hiding and the binding properties both statistical. Thus, either hiding or binding must be computational. A construction of statistically-binding scheme from any pseudorandom generator was given by Naor [23]. Since the existence of one-way functions is equivalent to that of pseudorandom generators [18], the statistically-binding scheme can be based on any one-way function. A construction of statistically-hiding scheme (NOVY scheme) from one-way permutation was given by Naor, Ostrovsky, Venkatesan and Yung [24]. After that, the assumption of the existence of one-way permutation was relaxed to that of approximable-preimage-size one-way function [12]. Finally, Haitner and Reingold [15] showed that a statistically-hiding scheme (HNORV scheme [13]) can be based on any one-way function.

Since statistically-binding (resp., statistically-hiding) bit commitment schemes are used as building block for zero-knowledge proof (resp., zero-knowledge argument) systems [10, 3], it is desirable to be efficient from several viewpoints (e.g., the total size of messages exchanged during the protocol, or the round number of communications in the protocol). In general, the round complexity of statistically-hiding schemes is large (see, e.g., [14, 11]).

Let us move on the quantum case. After the unconditionally security of the BB84 quantum key distribution protocol [2] was shown, the possibility of unconditionally secure quantum bit commitments had been investigated. Unfortunately, the impossibility of unconditionally secure quantum bit commitment was shown [21, 22]. After that, some relaxations such as quantum string commitment [19] or cheat-sensitive quantum bit commitment [1, 17, 4] have been studied.

In this paper, we take the computational approach as in the classical case. Along this line, Dumais, Mayers and Salvail [8] showed a construction of perfectly-hiding quantum bit commitment scheme (DMS scheme) based on quantum one-way permutation. The non-interactivity in DMS scheme is advantageous over the classical statistically-hiding bit commitments. Unfortunately, we have not found any candidate of quantum one-way permutation, because known candidates for classical one-way permutation are no longer one-way in the quantum setting due to Shor's algorithm [26]. Koshihara and Odaira [20] observed that the binding property of DMS scheme holds for any quantum one-way functions and showed that any approximable-preimage-size quantum one-way function suffices for the statistical hiding property.

In this paper, we further generalize statistically-hiding quantum bit commitment schemes in [8, 20] and show that a statistically-hiding quantum bit commitment is constructible from any *general* quantum one-way function without losing the non-interactivity. We basically follow the steps of the proof in [13]. Thus, we remark the similarity and differences.

- As in HNORV scheme [13], we consider to construct a 1-out-of-2 binding commitment scheme based on any quantum one-way function as an intermediate scheme. Our 1-out-of-2 binding commitment scheme executes in parallel two commitment schemes where one of the two commitment schemes satisfies the binding property and the other does not have to satisfy the binding property. Note that any adversary for the classical 1-out-of-2 binding commitment (of the serial composition) cannot see the second commitment just after getting the first commitment. But, in our case, the adversary can get both the first and the second commitments, which may be correlated. Thus, we have to cope with the adversary that can have more information. One of important technical tools in [13] is so-called “new interactive hashing theorem” [14]. We provides a quantum analogue of the new interactive hashing theorem.
- Since the resulting 1-out-of-2 binding commitment scheme satisfies the hiding property only in a weak sense, some hiding amplification technique is applied to yield a 1-out-of-2 binding commitment scheme with the hiding property in a strong sense. To this end, we just consider the repetitional use of quantum one-way function and show that the simple repetition works for the hiding amplification. In [13], an amplification procedure is recursively iterated and an iterative analysis is made. Due to the parallel composition, we can drastically simplify the security analysis of the hiding amplification.
- Finally, we construct a (normal) statistically-hiding quantum bit commitment from the 1-out-of-2 binding commitment scheme. Unlike HNORV scheme, we do not use, in this step, the technique of universal one-way hash functions, which requires interactions.

*Remark.* In the quantum setting, there are several definitions for the binding property of commitment schemes. In [7], a satisfactory definition is given. Nonetheless, we adopt a weaker definition as in [8] and construct a non-interactive quantum bit commitment scheme based on the weak definition. It seems much more difficult to prove the security of our construction according to the definition in [7] by using our techniques. I believe that the weak definition is sufficient for some applications. Actually, a construction of quantum oblivious transfer from a quantum string commitment (of a special type) with a similar weak binding condition was given in [6].

## 2 Preliminaries

### 2.1 Notations and Conventions

We denote the  $m$ -dimensional Hilbert space by  $H_m$ . Let  $\{|0\rangle, |1\rangle\}$  denote the computational basis for  $H_2$ . When the context requires, we write  $|b\rangle_+$  to denote  $|b\rangle$  in the computational basis. Let  $\{|0\rangle_\times, |1\rangle_\times\}$  denote the diagonal basis, where  $|0\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  and  $|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ . For any  $x = x_1x_2\cdots x_n \in \{0,1\}^n$  and  $\theta \in \{+, \times\}$ ,  $|x\rangle_\theta$  denotes the state  $\otimes_{i=1}^n |x_i\rangle_\theta$ . We denote  $|0\rangle \otimes \cdots \otimes |0\rangle$  by  $|\mathbf{0}\rangle$ . For projections, we denote  $\mathcal{P}_+^0 = |0\rangle\langle 0|$ ,  $\mathcal{P}_+^1 =$

$|1\rangle\langle 1|$ ,  $\mathcal{P}_\times^0 = |0\rangle_\times\langle 0|$ , and  $\mathcal{P}_\times^1 = |1\rangle_\times\langle 1|$ . For any  $x \in \{0,1\}^n$ , we denote  $\mathcal{P}_+^x = \otimes_{i=1}^n \mathcal{P}_+^{x_i}$  and  $\mathcal{P}_\times^x = \otimes_{i=1}^n \mathcal{P}_\times^{x_i}$ . For the sake of simplicity, we also write  $\mathcal{P}^x$  instead of  $\mathcal{P}_+^x$ . We define  $\theta(0) = +$  and  $\theta(1) = \times$ . Thus, for any  $w \in \{0,1\}$ ,  $\{\mathcal{P}_{\theta(w)}^x\}_{x \in \{0,1\}^n}$  is the von Neumann measurement. For density matrices  $\sigma$  and  $\rho$ , we define  $\delta(\sigma, \rho) \stackrel{\text{def}}{=} \|\sigma - \rho\|_1$ , where  $\|A\|_1 = \frac{1}{2}\text{tr}\sqrt{A^\dagger A}$ . For two classical random variables  $X$  and  $Y$ , there exists the corresponding density matrices  $\rho_X$  and  $\rho_Y$ . Since  $\delta(\rho_X, \rho_Y)$  also represents the variation distance (a.k.a. statistical distance) between  $X$  and  $Y$ , we sometimes write  $\delta(X, Y)$  instead of  $\delta(\rho_X, \rho_Y)$ . We denote the min-entropy of a random variable  $X$  by  $\mathbf{H}_\infty(X)$  and the Renyi entropy (of order 2) by  $\mathbf{H}_2(X)$ . We denote the uniform distribution over  $\{0,1\}^n$  by  $U_n$ . For a set  $A$ , we sometimes use the same symbol to denote the uniform distribution over the set  $A$ . A function  $\nu : \mathbb{N} \rightarrow \mathbb{R}$  is *negligible* if for every polynomial  $p$  there exists  $n_0 \in \mathbb{N}$  such for all  $n \geq n_0$ ,  $\nu(n) < 1/p(n)$ . We denote a set of integers  $\{i \in \mathbb{N} : n_1 \leq i \leq n_2\}$  by  $[n_1, n_2]$ .

## 2.2 Quantum One-Way Functions

In order to give definitions of quantum one-way functions, we have to decide a model of quantum computation. In this paper, we consider (uniform or non-uniform) quantum circuit family. As a universal quantum gate set, we take the controlled-NOT, the one-qubit Hadamard gate, and arbitrary one-qubit non-trivial rotation gate. The computational complexity of a circuit  $\mathcal{C}$  is measured by the number of elementary gates (in the universal gate set) contained in  $\mathcal{C}$  and denoted by  $\text{size}(\mathcal{C})$ . For any circuit family  $\mathcal{C} = \{\mathcal{C}_n\}_{n \in \mathbb{N}}$ , if  $\text{size}(\mathcal{C}_n)$  is bounded by  $p(n)$  for some polynomial  $p$ ,  $\mathcal{C}$  is called  $p$ -size circuit family.

Let  $f = \{f_n : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$  be a function family. To compute  $f$ , we need a circuit family  $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$  where  $\mathcal{C}_n$  is a circuit on  $m(n) \geq \ell(n)$  qubits. To compute  $f_n(x)$  for  $x \in \{0,1\}^n$ , we apply  $\mathcal{C}_n$  to  $|x\rangle \otimes |0\rangle^{\otimes m(n)-n}$ . The output of  $\mathcal{C}_n$  is obtained by the von Neumann measurement in the computational basis on  $\ell(n)$  qubits.

**Definition 2.1** A function family  $f = \{f_n : \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}\}_{n \in \mathbb{N}}$  is  $s(n)$ -secure quantum one-way if

- there exists a  $p$ -size circuit family  $\mathcal{C} = \{\mathcal{C}_n\}_{n \in \mathbb{N}}$  such that, for all  $n \geq 1$  and all  $x \in \{0,1\}^n$ ,  $\mathcal{C}_n(|x\rangle \otimes |0\rangle) = f_n(x)$  with certainty;
- for every  $p$ -size circuit family  $\mathcal{B} = \{\mathcal{B}_n\}_{n \in \mathbb{N}}$  and for sufficiently large  $n$ ,

$$\Pr[f_n(\mathcal{B}_n(f_n(U_n))) = f_n(U_n)] < 1/s(n).$$

If  $f$  is  $p(n)$ -secure quantum one-way for every polynomial  $p$ , then  $f$  is said to be  $p$ -secure.

Quantum one-way function  $f$  is said to be  $r(n)$ -regular if for any  $y \in \text{supp}(f(U_n))$ ,  $|\{x \in \{0,1\}^n : f_n(x) = y\}| = 2^{r(n)}$ . Without loss of generality, we can consider quantum one-way functions that are length-preserving, that is,  $\ell(n) = n$ , because general quantum one-way functions can be converted into ones that are length-preserving.

## 2.3 Quantum Bit Commitment

In a non-interactive quantum bit commitment scheme, honest Alice with her bit  $w \in \{0, 1\}$  starts with a system  $H_{\text{all}} = H_{\text{keep}} \otimes H_{\text{open}} \otimes H_{\text{commit}}$  in the initial state  $|0\rangle$ , executes a quantum circuit  $\mathcal{C}_{n,w}$  on  $|0\rangle$  returning the final state  $|\psi_w\rangle \in H_{\text{all}}$  and finally sends the subsystem  $H_{\text{commit}}$  to Bob in the reduced state  $\rho_B(w) = \text{tr}_A(|\psi_w\rangle\langle\psi_w|)$ , where Alice's Hilbert space is  $H_A = H_{\text{keep}} \otimes H_{\text{open}}$ . For  $w \in \{0, 1\}$ , we call  $\rho_B(w)$  *w-commitment state*. Once the system  $H_{\text{commit}}$  (or, *w-commitment state*) is sent to Bob, Alice has only access to  $\rho_A(w) = \text{tr}_B(|\psi_w\rangle\langle\psi_w|)$ , where Bob's Hilbert space is  $H_B = H_{\text{commit}}$ . To reveal the commitment, Alice needs only to send the system  $H_{\text{open}}$  together with  $w$ . Bob then checks the value of  $w$  by measuring the system  $H_{\text{open}} \otimes H_{\text{commit}}$  with some measurement that is fixed by the protocol in view of  $w$ . Bob obtains  $w = 0$ ,  $w = 1$ , or  $w = \perp$  when the value of  $w$  is rejected.

Cheating Alice must start with the state  $|0\rangle$  of some system  $H_{\text{all}} = H_{\text{extra}} \otimes H_A \otimes H_{\text{commit}}$ . A quantum circuit  $\mathcal{D}_n$  that acts on  $H_{\text{all}}$  is executed to obtain a state  $|\psi\rangle$  and the subsystem  $H_{\text{commit}}$  is sent to Bob. Later, any quantum circuit  $\mathcal{O}_n$  which acts on  $H_{\text{extra}} \otimes H_{\text{keep}} \otimes H_{\text{open}}$  can be executed before sending the subsystem  $H_{\text{open}}$  to Bob. The important quantum circuits which act on  $H_{\text{extra}} \otimes H_{\text{keep}} \otimes H_{\text{open}}$  are the quantum circuits  $\mathcal{O}_{n,0}$  (resp.,  $\mathcal{O}_{n,1}$ ) which maximizes the probability that bit  $w = 0$  (resp.,  $w = 1$ ) is revealed with success. Therefore, any attack can be modeled by triplets of quantum circuits  $\{(\mathcal{D}_n, \mathcal{O}_{n,0}, \mathcal{O}_{n,1})\}_{n \in \mathbb{N}}$ .

Let  $b_0(n)$  (resp.,  $b_1(n)$ ) be the probability that she succeeds to reveal 0 (resp., 1) using the corresponding optimal circuit  $\mathcal{O}_{n,0}$  (resp.,  $\mathcal{O}_{n,1}$ ). The definition of  $b_w(n)$  explicitly requires that the value of  $w$ , which cheating Alice tries to open, is chosen not only before the execution of the measurement on  $H_{\text{open}} \otimes H_{\text{commit}}$  by Bob but also before the execution of the circuit  $\mathcal{O}_{n,w}$  by cheating Alice.

In the quantum setting, it is pointed out in [22] that the requirement “ $b_0(n) = 0 \vee b_1(n) = 0$ ” for the binding condition is too strong. Thus, we adopt a weaker condition  $b(n) \stackrel{\text{def}}{=} b_0(n) + b_1(n) - 1 \leq \varepsilon$  where  $\varepsilon(n)$  is negligible, which is the same condition as in [8].

Since we consider the computational binding, we modify the above discussion so as to fit the computational setting. Instead of the triplet  $(\mathcal{D}_n, \mathcal{O}_{n,0}, \mathcal{O}_{n,1})$ , we consider a pair  $(\mathcal{D}_{n,0}, \mathcal{U}_n)$ . If we set  $\mathcal{D}_{n,0} = (\mathcal{O}_{n,0} \otimes \mathcal{I}_{\text{commit}}) \cdot \mathcal{D}_n$ , and  $\mathcal{U}_n = \mathcal{O}_{n,1} \cdot \mathcal{O}_{n,0}^\dagger$ , we can easily see that the adversary's strategy does not change. Note that  $\mathcal{D}_{n,0}$  acts in  $H_{\text{all}}$  and  $\mathcal{U}_n$  is restricted to act only in  $H_{\text{extra}} \otimes H_{\text{keep}} \otimes H_{\text{open}}$ .

**Definition 2.2** A non-interactive quantum bit commitment is *t(n)-computationally-binding* if, for every a family  $\{(\mathcal{D}_{n,0}, \mathcal{U}_n)\}_{n \in \mathbb{N}}$  of p-size circuit pairs,  $b(n)$  is bounded by  $t(n)$ . If  $t(n)$  is negligible in  $n$ , the non-interactive quantum bit commitment is simply said to be *computationally-binding*.

**Definition 2.3** A non-interactive quantum bit commitment is *t(n)-statistically-binding* if  $b(n) \leq t(n)$ . If  $t(n)$  is negligible in  $n$ , the non-interactive quantum bit commitment is simply said to be *statistically-hiding*.

As mentioned, a satisfactory definition for the binding property of quantum bit commitment schemes is given by Damgård, Fehr, Renner, Salvail and Schaffner [7]. Actually, they show that a variant of DMS scheme satisfies the binding condition in [7]. However, it is still unclear whether the inverting quantum one-way permutation is reducible to violating the binding condition. We rather adopt a weaker definition in [8] in order to benefit from the computational reducibility.

## 2.4 Pairwise Independent Hash Functions

Let  $H = \{H_n\}_{n \in \mathbb{N}}$  be a sequence of function families, where each  $H_n$  is a family of functions mapping binary strings of length  $\ell(n)$  to strings of length  $v(n)$ . We say that  $H_n$  is a *pairwise independent* (a.k.a. strongly 2-universal) *hash family* if for any distinct  $x, x' \in \{0, 1\}^{\ell(n)}$  and  $y, y' \in \{0, 1\}^{v(n)}$ ,  $\Pr_{h \leftarrow H_n}[h(x) = y \wedge h(x') = y'] = 2^{-2v(n)}$ . (See, e.g., [5] for an implementation of pairwise independent hash family.)

One of the useful applications of pairwise independent hash family is smoothing the min-entropy of given distribution.

**Lemma 2.1** (*Leftover Hash Lemma*) *Let  $V_n$  be a random variable over  $\{0, 1\}^{\ell(n)}$  such that  $H_\infty(V_n) \geq \lambda_n$  and  $H_n$  be a pairwise independent hash family where each  $h \in H_n$  maps strings of length  $\ell(n)$  to strings of length  $\lambda_n - 2 \log(\varepsilon^{-1})$ . Then, we have  $\delta((H_n, H_n(V_n)), (H_n, U_{v(n)})) \leq \varepsilon$ .*

## 3 Base Scheme

Dumais, Mayers and Salvail [8] gave a non-interactive statistically-hiding quantum bit commitment based on quantum one-way permutation. Koshiha and Odaira [20] observed that DMS scheme still satisfies the computational binding if we replace quantum one-way permutation with general quantum one-way function. So, we consider to use the scheme as an important ingredient of the construction of our non-interactive statistically-hiding quantum bit commitment based on quantum one-way function.

We briefly review the scheme. Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be a function family. The quantum bit commitment scheme takes the security parameter  $n$  and the description of function family  $f$  as common inputs. For given  $f$  and the security parameter  $n$ , Alice and Bob determine  $f_n$ . The protocol, called **Base Protocol**, is described in Figure 1.

**Proposition 3.1** (Implicit in [8] and explicit in [20]) *Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be a family of (not necessarily quantum one-way) functions such that  $\delta(f(U_n), U'_n)$  is negligible in  $n$ . Then, Base Protocol is statistically hiding.*

**Proposition 3.2** (Implicit in [8] and explicit in [20]) *Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be an  $s(n)$ -secure quantum one-way function family. Then Base Protocol is  $O(1/\sqrt{s(n)})$ -computationally binding.*

---

**Commit Phase:**

1. Alice with her bit  $w$  first chooses  $x \in \{0, 1\}^n$  uniformly and computes  $y = f_n(x)$ .
2. Next, Alice sends the quantum state  $|f_n(x)\rangle_{\theta(w)} \in \mathbf{H}_{\text{commit}}$  to Bob.
3. Bob then stores the received quantum state until Reveal Phase.

**Reveal Phase:**

1. Alice first announces  $w$  and  $x$  to Bob.
  2. Next, Bob measures  $\rho_B$  with measurement  $\{P_{\theta(w)}^y\}_{y \in \text{range}(f_n)}$  and obtains the classical output  $y' \in \text{range}(f_n)$ .
  3. Lastly, Bob accepts if and only if  $y' = f_n(x)$ .
- 

Figure 1: Base Protocol

In this paper, we do not use directly the above properties. We need to generalize Proposition 3.2. In non-interactive commitment protocols, Alice sends a commitment  $y$  in Commit Phase and a decommitment  $x$  in Reveal Phase. To make Bob accept, the pair  $(y, x)$  must be in some binary relation  $R_n$ . In case of **Base Protocol**, the binary relation is defined as  $R_n = \{(f_n(x), x) : x \in \{0, 1\}^n\}$ . We can rephrase the statement of Proposition 3.2 in terms of the binary relation  $R_n$ . It says that if cheating Alice can output distinct pairs  $(y, x)$  and  $(y', x')$  both in  $R_n$  such that the probability to reveal 0 with success by using  $(x, y)$  is  $b_0(n)$ , the probability to reveal 1 with success by using  $(x', y')$  is  $b_1(n)$ , and  $b_0(n) + b_1(n) \geq 1 + \sqrt{s(n)}$ , then there exists an algorithm that, given  $f_n(x)$  as input, outputs  $x$  such that  $(f_n(x), x) \in R_n$  with probability  $\Omega(s(n))$ . Since **Base Protocol** is based on quantum one-way function, the definition of  $R_n$  is quite natural. On the other hand, we may define a binary relation as  $R'_n = \{(f_n(x), x) : x \in W_n\}$  by using some subset  $W_n \subseteq \{0, 1\}^n$ . We discuss a generalization of Proposition 3.2 in the next section.

## 4 Non-interactive Quantum Hashing Theorem

The following theorem is a quantum correspondence<sup>1</sup> of the new interactive hashing theorem in [14] and it is one of the most technical ingredients in this paper.

**Theorem 4.1** (*Non-interactive Quantum Hashing Theorem*) *Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be an  $s(n)$ -secure quantum one-way function family. Suppose that  $W_n$  is a subset of  $\{0, 1\}^n$  and define the binary relation  $R'_n$  as  $R'_n = \{(f_n(x), x) : x \in W_n\}$ . If there exists an algorithm*

---

<sup>1</sup>Exactly speaking, Theorem 4.1 corresponds to a special case of the new interactive hashing theorem in [14] and the current form suffices for our purpose. As in [14], we can derive a more general form of Non-interactive Quantum Hashing Theorem.

against Base Protocol that can output distinct pairs  $(y, x)$  and  $(y', x')$  both in  $R'_n$  such that the probability to reveal 0 with success by using  $(x, y)$  is  $b_0(n)$ , the probability to reveal 1 with success by using  $(x', y')$  is  $b_1(n)$ , and  $b_0(n) + b_1(n) \geq 1 + \sqrt{s(n)}$ , then there exists another algorithm that, given  $y'' \in f_n(W_n)$  as input, outputs  $x''$  such that  $(y'', x'') \in R'_n$  with probability  $\Omega(s(n))$ , where  $y''$  is proportionally selected from  $f_n(W_n)$ .

If  $W_n$  is closed to  $U_n$  in the statement above, Non-interactive Quantum Hashing Theorem can be directly applied to construct an inverter of the quantum one-way function as in [8, 20]. However, if  $W_n$  is far from  $U_n$ , it is not directly related to the inversion of the quantum one-way function. In the next section, we discuss how to use it even in the case where  $W_n$  is far from  $U_n$ .

For the proof of Theorem 4.1, we can adapt the proof of Proposition 3.2. In the original proof in [8] of Proposition 3.2, some “test circuits” are utilized. The existence of test circuits is an obstacle to the generalization. A careful analysis shows that such test circuits are redundant.

**Proof.** We separate the whole system into three parts: the system  $H_{\text{commit}}$  that encodes the functional value, the system  $H_{\text{open}}$  that encodes inputs to the function, and the system  $H_{\text{keep}}$  is the reminder of the system.

#### Perfect Case:

In the perfect case, we can assume that an adversary  $\{\mathcal{D}_{n,0}, \mathcal{U}_n\}_{n \in \mathbb{N}}$  reveals the committed bit in both ways perfectly. That is, the states  $|\psi_{n,0}\rangle$  (resp.,  $|\psi_{n,1}\rangle$ ) of the whole system when  $w = 0$  (resp.,  $w = 1$ ) will be committed can be written as follows.

$$\begin{aligned} |\psi_{n,0}\rangle &= \sum_{x \in W_n} |\alpha_{0,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle_+^{\text{commit}} = \mathcal{D}_{n,0}|\mathbf{0}\rangle \quad \text{and} \\ |\psi_{n,1}\rangle &= \sum_{x \in W_n} |\alpha_{1,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle_{\times}^{\text{commit}} = \mathcal{U}_n|\psi_{n,0}\rangle, \end{aligned}$$

where  $\sum_{x \in W_n} \|\alpha_{0,x}\|^2 = \sum_{x \in W_n} \|\alpha_{1,x}\|^2 = 1$ .

Let  $\mathcal{P}_+^{u,\text{commit}}$  and  $\mathcal{P}_{\times}^{u,\text{commit}}$  be the projection operators  $\mathcal{P}_+^u$  and  $\mathcal{P}_{\times}^u$  respectively, acting in  $H_{\text{commit}}$ . We are interested in properties on the state  $|\varphi_{n,0}^u\rangle = \mathcal{P}_{\times}^{u,\text{commit}}|\psi_{n,0}\rangle$  which plays an important role for the inverter.

Now we consider an algorithm to invert  $y \in f_n(W_n)$ . Thus, we assume that  $y$  is encoded as input to the inverter in  $H_{\text{inv}}$ . Before considering the inverter, we consider properties on the states  $|\varphi_{n,0}^u\rangle$  for every  $u \in \{0, 1\}^n$ :

1.  $\|\varphi_{n,0}^u\|^2 = 2^{-n/2}$ ;
2. there exists an efficient circuit  $\mathcal{W}_n$  on  $H_{\text{inv}} \otimes H_{\text{open}} \otimes H_{\text{commit}}$  which if  $u$  is in  $H_{\text{inv}}$ , unitarily maps  $|\psi_{n,0}\rangle$  to  $2^{n/2}|\varphi_{n,0}^u\rangle$ ;
3.  $\mathcal{U}_n|\varphi_{n,0}^u\rangle = \sum_{z \in f_n^{-1}(u)} |\alpha_{1,z}\rangle^{\text{keep}} \otimes |z\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}}$ .



If the above properties are true, we can consider an inverter as follows. On input  $y$ , the inverter generates the state  $|\psi_{n,0}\rangle$  by applying  $\mathcal{D}_{n,0}$  to  $|\mathbf{0}\rangle$ , then applies  $\mathcal{W}_n$  and  $\mathcal{U}_n$  in order, and finally measures  $\mathbf{H}_{\text{open}}$  to obtain  $z \in f_n^{-1}(y)$ .

In what follows, we show each property is true. First, we show Property 1. We write  $|\psi_{n,0}\rangle$  using the diagonal basis for  $\mathbf{H}_{\text{commit}}$ , and then we have

$$\begin{aligned} |\psi_{n,0}\rangle &= \sum_{x \in W_n} |\alpha_{0,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes \left( \sum_{u \in \{0,1\}^n} \frac{(-1)^{\langle u, f_n(x) \rangle}}{2^{n/2}} |u\rangle_{\times}^{\text{commit}} \right) \\ &= 2^{-n/2} \sum_{\substack{u \in \{0,1\}^n \\ x \in W_n}} (-1)^{\langle u, f_n(x) \rangle} |\alpha_{0,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}}. \end{aligned}$$

Since

$$|\varphi_{n,0}^u\rangle = 2^{-n/2} \sum_{x \in W_n} (-1)^{\langle u, f_n(x) \rangle} |\alpha_{0,x}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}},$$

Property 1 holds. Next, we consider Property 3. Since the state  $|\psi_{n,1}\rangle$  can be written as

$$|\psi_{n,1}\rangle = \sum_{u \in f_n(W_n)} \left( \sum_{z \in f_n^{-1}(u)} |\alpha_{1,z}\rangle^{\text{keep}} \otimes |z\rangle^{\text{open}} \right) \otimes |u\rangle_{\times}^{\text{commit}},$$

it implies that for every  $u \in f_n(W_n)$

$$\begin{aligned} \mathcal{U}_n |\varphi_{n,0}^u\rangle &= \mathcal{U}_n \mathcal{P}_{\times}^{u, \text{commit}} |\psi_{n,0}\rangle = \mathcal{P}_{\times}^{u, \text{commit}} \mathcal{U}_n |\psi_{n,0}\rangle \\ &= \mathcal{P}_{\times}^{u, \text{commit}} |\psi_{n,1}\rangle = \sum_{z \in f_n^{-1}(u)} |\alpha_{1,z}\rangle^{\text{keep}} \otimes |z\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}}. \end{aligned}$$

(Note that  $\mathcal{U}_n$  is restricted to act in  $\mathbf{H}_{\text{keep}} \otimes \mathbf{H}_{\text{open}}$  and thus  $\mathcal{U}_n$  and  $\mathcal{P}_{\times}^{u, \text{commit}}$  are commutable.) Thus, Property 3 holds. Finally, we consider Property 2. We describe how to implement  $\mathcal{W}_n$  mapping from

$$|u\rangle^{\text{inv}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle_+^{\text{commit}}$$

into

$$(-1)^{\langle u, f_n(x) \rangle} |u\rangle^{\text{inv}} \otimes |x\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}}$$

for every  $u \in f_n(W_n)$ , which satisfies the requirement. First we apply the mapping  $|u\rangle^{\text{inv}} \otimes |f_n(x)\rangle_+^{\text{commit}} \mapsto (-1)^{\langle u, f_n(x) \rangle} |u\rangle^{\text{inv}} \otimes |f_n(x)\rangle_+^{\text{commit}}$ , which can be efficiently implemented by using the Hadamard gate and the controlled-NOT gate. Secondly, we apply the mapping  $|x\rangle^{\text{open}} \otimes |u\rangle_{\times}^{\text{commit}} \mapsto |x\rangle^{\text{open}} \otimes |u \oplus f_n(x)\rangle_+^{\text{commit}}$ , which can be implemented by the efficient evaluation circuit of  $f_n$ . Thirdly, we apply the mapping  $|y\rangle^{\text{inv}} \otimes |u\rangle_{\times}^{\text{commit}} \mapsto |y\rangle^{\text{inv}} \otimes |y \oplus u\rangle_+^{\text{commit}}$ , which can be efficiently implemented by using the controlled-NOT gate. Finally, we apply the Hadamard gate to the all qubits in  $\mathbf{H}_{\text{commit}}$ . It is easy to verify that the above procedure satisfies the requirement. Thus, Property 2 holds.

**General Case:**

In the general case, the states  $|\tilde{\psi}_{n,0}\rangle = \mathcal{D}_{n,0}|\mathbf{0}\rangle$  and  $|\tilde{\psi}_{n,1}\rangle = \mathcal{U}_n|\tilde{\psi}_{n,0}\rangle$  can be generally written as

$$\begin{aligned} |\tilde{\psi}_{n,0}\rangle &= \sum_{x \in \{0,1\}^n, y \in \{0,1\}^n} |\alpha_{0,x,y}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |y\rangle_+^{\text{commit}}, \quad \text{and} \\ |\tilde{\psi}_{n,1}\rangle &= \sum_{x \in \{0,1\}^n, y \in \{0,1\}^n} |\alpha_{1,x,y}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |y\rangle_{\times}^{\text{commit}}, \end{aligned}$$

where  $\sum_{x,y} \|\alpha_{0,x,y}\|^2 = \sum_{x,y} \|\alpha_{1,x,y}\|^2 = 1$ .

We assume that  $b_0(n) + b_1(n) \geq 1 + 1/p(n)$  for some polynomial  $p$ , where

$$b_0(n) = \sum_{x \in W_n} \|\alpha_{0,x,f_n(x)}\|^2 \quad \text{and} \quad b_1(n) = \sum_{x \in W_n} \|\alpha_{1,x,f_n(x)}\|^2.$$

Then we will show that the success probability  $p_{\text{inv}}$  for inverting the underlying quantum one-way function is greater than  $1/4(p(n))^2$ .

First, the state  $|\tilde{\psi}_{n,0}\rangle$  can be written as follows.

$$\begin{aligned} |\tilde{\psi}_{n,0}\rangle &= \sum_{x \in W_n} |\alpha_{0,x,f_n(x)}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle^{\text{commit}} \\ &\quad + \sum_{f_n(x) \neq z \text{ or } x \notin W_n} |\alpha_{0,x,z}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |z\rangle^{\text{commit}}. \end{aligned}$$

Remember that the state in the perfect case can be written as

$$|\psi_{n,0}\rangle = \sum_{x \in W_n} |\alpha_{x,0}\rangle^{\text{keep}} \otimes |x\rangle^{\text{open}} \otimes |f_n(x)\rangle^{\text{commit}}.$$

Then we have

$$|\alpha_{0,x}\rangle^{\text{keep}} = (b_0(n))^{-1/2} |\alpha_{0,x,f_n(x)}\rangle^{\text{keep}} \quad \text{and} \quad b_0(n) = \sum_{x \in W_n} \|\alpha_{0,x,f_n(x)}\|^2 = |\langle \psi_{n,0} | \tilde{\psi}_{n,0} \rangle|^2.$$

On input  $y$ , the inverter generates the state  $|\tilde{\psi}_{n,0}\rangle$  by applying  $\mathcal{D}_{n,0}$  to  $|\mathbf{0}\rangle$ . We then apply in order  $\mathcal{W}_n$  and  $\mathcal{U}_n$  to the resulting state and finally measures  $\mathbf{H}_{\text{open}}$  to hopefully obtain  $z \in f_n^{-1}(y)$ .

We have to estimate the success probability of the inverter. To this end, we define two projections:

$$\begin{aligned} \mathcal{P}_0 &\stackrel{\text{def}}{=} \sum_{x \in W_n} \mathcal{P}^{x,\text{open}} \otimes \mathcal{P}_+^{f_n(x),\text{commit}} \quad \text{and} \\ \mathcal{P}_1 &\stackrel{\text{def}}{=} \sum_{x \in W_n} \mathcal{P}^{x,\text{open}} \otimes \mathcal{P}_{\times}^{f_n(x),\text{commit}}. \end{aligned}$$

Then we have  $b_0(n) = \|\mathcal{P}_0|\tilde{\psi}_{n,0}\rangle\|^2$  and  $b_1(n) = \|\mathcal{P}_1|\tilde{\psi}_{n,1}\rangle\|^2$ . Here, we claim that the success probability  $p_{\text{inv}}$  satisfies

$$p_{\text{inv}} = \|\mathcal{P}_1 \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle\|^2.$$

We will see this claim. As mentioned, the state is  $|y\rangle^{\text{inv}} \otimes |\psi_{n,0}\rangle$  with probability  $\|\mathcal{P}_0|\tilde{\psi}_{n,0}\rangle\|^2 = b_0(n)$ , where  $y$  is the input to the inverter. As we see in the perfect case,  $\mathcal{W}_n$  maps the state  $|\psi_{n,0}\rangle$  into  $2^{n/2}|\varphi_{n,0}^y\rangle = 2^{n/2}\mathcal{P}_\times^{y,\text{commit}}|\psi_{n,0}\rangle$ . After that, we apply  $\mathcal{U}_n$  and measure  $\mathbf{H}_{\text{open}}$ . Thus, the success probability  $p_{\text{inv}}(y)$  for input  $y$  is written as

$$\begin{aligned} p_{\text{inv}}(y) &= b_0(n)2^n \left\| \left( \sum_{z \in f_n^{-1}(y)} \mathcal{P}^{z,\text{open}} \right) \mathcal{P}_\times^{y,\text{commit}} \mathcal{U}_n |\psi_{n,0}\rangle \right\|^2 \\ &= 2^n \left\| \left( \sum_{z \in f_n^{-1}(y)} \mathcal{P}^{z,\text{open}} \right) \mathcal{P}_\times^{y,\text{commit}} \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle \right\|^2. \end{aligned}$$

Averaging over all value according to the output distribution of  $f_n$ , we have

$$\begin{aligned} p_{\text{inv}} &= \sum_{y \in f_n(W_n)} \Pr[y = f_n(U_n)] p_{\text{inv}}(y) \\ &= \sum_{y \in f_n(W_n)} \left\| \left( \left( \sum_{z \in f_n^{-1}(y)} \mathcal{P}^{z,\text{open}} \right) \otimes \mathcal{P}_\times^{y,\text{commit}} \right) \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle \right\|^2 \\ &= \left\| \left( \sum_{y \in f_n(W_n)} \left( \left( \sum_{z \in f_n^{-1}(y)} \mathcal{P}^{z,\text{open}} \right) \otimes \mathcal{P}_\times^{y,\text{commit}} \right) \right) \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle \right\|^2 \\ &= \|\mathcal{P}_1 \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle\|^2. \end{aligned}$$

Furthermore, we rewrite the above to easily estimate the value of  $p_{\text{inv}}$ .

$$\begin{aligned} p_{\text{inv}} &= \|\mathcal{P}_1 \mathcal{U}_n \mathcal{P}_0 |\tilde{\psi}_{n,0}\rangle\|^2 = \|\mathcal{P}_1 \mathcal{U}_n (\mathcal{I} - \mathcal{P}_0^\perp) |\tilde{\psi}_{n,0}\rangle\|^2 \\ &= \|\mathcal{P}_1 \mathcal{U}_n |\tilde{\psi}_{n,0}\rangle - \mathcal{P}_1 \mathcal{U}_n \mathcal{P}_0^\perp |\tilde{\psi}_{n,0}\rangle\|^2 \\ &= \|\mathcal{P}_1 |\tilde{\psi}_{n,1}\rangle - \mathcal{P}_1 \mathcal{U}_n \mathcal{P}_0^\perp |\tilde{\psi}_{n,0}\rangle\|^2. \end{aligned}$$

Using the triangle inequality and  $b_1(n) > 1 - b_0(n)$ , we have

$$\begin{aligned} p_{\text{inv}} &\geq \left( \|\mathcal{P}_1 |\tilde{\psi}_{n,1}\rangle\| - \|\mathcal{P}_1 \mathcal{U}_n \mathcal{P}_0^\perp |\tilde{\psi}_{n,0}\rangle\| \right)^2 \\ &\geq \left( \|\mathcal{P}_1 |\tilde{\psi}_{n,1}\rangle\| - \|\mathcal{P}_0^\perp |\tilde{\psi}_{n,0}\rangle\| \right)^2 \\ &= \left( \sqrt{b_1(n)} - \sqrt{1 - b_0(n)} \right)^2. \end{aligned}$$

Let us recall that we assume that  $b_0(n) + b_1(n) > 1 + 1/p(n)$  for some polynomial  $p$ . After some calculation, we have

$$p_{\text{inv}} \geq 2 - 1/p - 2\sqrt{1 - 1/p} \geq 1/4(p(n))^2.$$

This completes the proof of Theorem 4.1.  $\square$

## 5 1-out-of-2 binding commitment from quantum one-way function

A 1-out-of-2 binding (we denote by  $\binom{2}{1}$ -binding) commitment scheme consists of two commitment schemes where one of the two commitment schemes satisfies the binding property and the other does not have to satisfy the binding property. In [13], Haitner *et al.* introduced a notion of 1-out-of-2 binding commitment schemes and gave a construction of  $\binom{2}{1}$ -binding commitment schemes based on one-way function. We also consider a quantum version of  $\binom{2}{1}$ -binding commitment scheme and construct a  $\binom{2}{1}$ -binding quantum commitment scheme.

We define a *2-parallel quantum bit commitment scheme*  $\Pi = (\Pi_1, \Pi_2)$ , which is a parallel composition of two non-interactive quantum bit commitment schemes  $\Pi_1$  and  $\Pi_2$ . At the beginning of the protocol  $\Pi$ , Alice has two bits  $w_1$  and  $w_2$ .  $\Pi$  consists of two phases, Commit Phase and Reveal Phase, as the standard bit commitment schemes do. In Commit Phase, Alice (in  $\Pi$ ) invokes Commit Phase of  $\Pi_1$  and sends  $w_1$ -commitment state (of  $\Pi_1$ ) to Bob. Also she invokes Commit Phase of  $\Pi_2$  and sends  $w_2$ -commitment state (of  $\Pi_2$ ) to Bob. We call the joint state of the  $w_1$ -commitment state (of  $\Pi_1$ ) and the  $w_2$ -commitment state (of  $\Pi_2$ )  $(w_1, w_2)$ -commitment state (of  $\Pi$ ). In Reveal phase, Alice sends decommitments both of  $\Pi_1$  and  $\Pi_2$ . Bob accepts if the both decommitments are valid.

Next, we would like to define “computational 1-out-of-2 binding”. In the classical case, it is defined in terms of transcripts. In the quantum case, the definition based on transcripts is not easy to handle with. Fortunately, our protocol below has a classical inner-state which controls the 1-out-of-2 binding property. Thus, after providing our protocol, we will give a protocol-specific definition of computational 1-out-of-2 binding. Moreover, we discuss the hiding property later.

We give our 2-parallel quantum bit commitment protocol (called **Protocol 1**) in Figure 2. While a sequential composition is discussed in [13], our protocol runs **Base Protocol** twice in parallel.

**Definition 5.1** *Protocol 1 is computationally 1-out-of-2-binding if there exists a set  $S \subseteq \{0, 1\}^n$  such that for every function  $\varepsilon(n) = 1/\text{poly}(n)$ , the first half of the 2-parallel quantum bit commitment is  $\varepsilon(n)$ -computationally-binding on condition that a randomly chosen  $x$  falls into  $S$  and the second half is  $\varepsilon(n)$ -statistically-binding on condition that  $x$  does not fall into  $S$ .*

Next, we define the hiding property. Unfortunately, the hiding property of **Protocol 1** is not so strong. This is because the preimage-size of  $f$  is not constant over the inputs. Thus, we consider the following weak definition of the binding property.

**Definition 5.2** *If, for any  $\gamma$  with  $0 \leq \gamma \leq 1$ , there exists a subset  $\Gamma \subseteq \{0, 1\}^n$  satisfying the following two properties, then 2-parallel quantum bit commitment is  $\gamma$ -hiding.*

---

**Parameters:** Integers  $t \in [1, n]$ ,  $\Delta_1 \in [0, t]$  and  $\Delta_2 \in [0, n - t]$ .

**Commit Phase:**

1. Alice with her two bits  $w_1$  and  $w_2$  first chooses  $x \in \{0, 1\}^n$  uniformly and computes  $y = f_n(x)$ . She also randomly chooses two hash functions  $h_1$  and  $h_2$  from families of pairwise independent hash functions  $H^{(1)} = \{h_1 : \{0, 1\}^n \rightarrow \{0, 1\}^{t-\Delta_1}\}$  and  $H^{(2)} = \{h_2 : \{0, 1\}^n \rightarrow \{0, 1\}^{n-t-\Delta_2}\}$ , respectively.
2. Next, Alice sends the quantum state

$$|h_1, h_1(y)\rangle_{\theta(w_1)} \otimes |h_2, h_2(x)\rangle_{\theta(w_2)} \in \mathbf{H}_{\text{commit}_1} \otimes \mathbf{H}_{\text{commit}_2}$$

to Bob.

3. Bob then stores the received quantum state  $\rho_B$  until the reveal phase.

**Reveal Phase:**

1. Alice announces the first decommitment  $(w_1, h_1, y)$  and the second decommitment  $(w_2, h_2, x)$  to Bob.
  2. Next, Bob measures the first register of  $\rho_B$  with measurement  $\{P_{\theta(w_1)}^{h,z}\}_{h \in H^{(1)}, z \in \text{range}(h_1)}$  and obtains the classical output  $(h, z) \in H^{(1)} \times \text{range}(h_1)$ . Also he simultaneously measures the second register with measurement  $\{P_{\theta(w_2)}^{h',z'}\}_{h' \in H^{(2)}, z' \in \text{range}(h_2)}$  and obtains the classical output  $(h', z') \in H^{(2)} \times \text{range}(h_2)$ .
  3. Lastly, Bob accepts the first commitment if and only if  $h(y) = z$ . Also he accepts the second commitment if and only if  $h'(z') = x$  and  $y = f_n(x)$ .
- 

Figure 2: Protocol 1

1.  $|\Gamma| \geq \gamma \cdot 2^n$ .
2. Let  $w_1, w_2 \in \{0, 1\}$ . Let  $Z_1(w_1)$  be a random variable for the first half of the commitment when  $w_1$  is the first bit to be committed and  $Z_2(w_2)$  be a random variable for the second half when  $w_2$  is the second bit to be committed, on condition that  $x$  is uniformly chosen from  $\Gamma$ . Namely, the value for  $(Z_1, Z_2)$  takes  $|h, h(f_n(x))\rangle_{\theta(w_1)} \otimes |h', h'(x)\rangle_{\theta(w_2)}$  where  $h$  is uniformly chosen from  $H^{(1)}$ ,  $h'$  is uniformly chosen from  $H^{(2)}$  and  $x$  is uniformly chosen from  $\Gamma$ . Then,  $(Z_1(0), Z_2(0))$ ,  $(Z_1(0), Z_2(1))$ ,  $(Z_1(1), Z_2(0))$  and  $(Z_1(1), Z_2(1))$  are negligibly close to each other.

**Theorem 5.1** *Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be an  $s(n)$ -secure regular quantum one-way function family, where  $s(n) = n^{\omega(1)}$ . Then Protocol 1 with setting of parameters  $\Delta_1 = \Delta_2 = \frac{1}{4} \log s(n)$ , is a 2-parallel quantum bit commitment scheme that is computationally 1-out-of-2 binding, regardless of the setting of  $t$ .*

While HNORV scheme is two sequential of commitment schemes, ours is two parallel of quantum commitment schemes. Thus, we have to take into the account that the second half of the commitment might increase the power of the adversary. Fortunately, such information can be included in the adversary's private space  $\mathbf{H}_{\text{keep}}$  and we can use the same reduction as in Base Protocol. Actually, this observation plays an important role through the paper. Moreover, there is another difficulty in the analysis. Since the computational property of  $\binom{2}{1}$ -binding commitment is conditional (i.e.,  $x \in S$ ), we have to consider the reduction between two algorithms whose input distributions are different. To overcome the difficulty, we use Non-interactive Quantum Hashing Theorem. While the proof of the computational part is similar to the proof in [13], the proof of the statistical part is completely different from the proof in [13] because it involves the analysis of quantum states.

**Proof.** For every  $t \in [1, n]$ , we define the set of “heavy” strings to be

$$S_t = \{x \in f_n^{-1}(y) : \Pr[f_n(U_n) = y] \geq 2^{-t-\Delta_3}\}$$

for the parameter  $\Delta_3 = \frac{1}{2}s(n)$ .

We will show that if  $x \in S_t$  is chosen in the first step of Commit Phase then the first half is binding and if  $x \notin S_t$  then the second half is binding.

First, we show a reduction from inverting  $f_n$  to violating the binding property of Protocol 1 in the case of  $x \in S_t$ . Let  $f'_n : H^{(1)} \times \{0, 1\}^n \rightarrow H^{(1)} \times \{0, 1\}^{t-\Delta_1}$  be a function that maps  $(h, x)$  to  $(h, h(f_n(x)))$ . We define  $R'_n = \{(f'_n(h, x), (h, x)) : x \in S_t \text{ and } h \in H^{(1)}\}$  and  $W_{h, \eta} = \{x \in \{0, 1\}^n : (\eta, (h, x)) \in R'_n\}$ .

Let  $\mathcal{A}_1$  be a quantum algorithm to violate the binding property (with respect to  $R'_n$ ) of Protocol 1 with probability  $\varepsilon(n)$ . Then, from Theorem 4.1, we have another algorithm  $\mathcal{A}_2$  that inverts  $f'_n(h, x)$ . Namely,

$$\Pr[\mathcal{A}_2(H^{(1)}, H^{(1)}(f_n(U_n))) \in W_{H^{(1)}, H^{(1)}(f_n(U_n))}] \geq \varepsilon(n)^2/4.$$

For each  $h \in H^{(1)}$  and  $x \in \{0, 1\}^n$ , we consider

$$p_{h,x} = \frac{\Pr[\mathcal{A}_2(f'_n(h, x)) \in W_{h,h(f_n(x))}]}{|f_n'^{-1}(f'_n(h, x))|}$$

and set

$$T = \{(h, x) : p_{h,x} \geq \frac{\varepsilon(n)^2}{8}\}.$$

By the counting argument, we have  $|T| \geq \varepsilon^2(n)/8 \cdot 2^n |H^{(1)}|$ . Here, we estimate the following probability:

$$\begin{aligned} & \Pr[\mathcal{A}_2(H^{(1)}, U_{t-\Delta_1}) \in W_{H^{(1)}, U_{t-\Delta_1}}] \\ & \geq \sum_{(h,x) \in T} \Pr[\mathcal{A}_2(h, h(f_n(x))) \in W_{h,h(f_n(x))}] \cdot \Pr[H^{(1)} = h \wedge U_{t-\Delta_1} = h(f_n(x))] \\ & \geq \varepsilon^4(n)/64. \end{aligned}$$

We consider an algorithm  $\mathcal{B}$  that on input  $y = f_n(x)$ , picks randomly a hash function  $h \in H^{(1)}$ , and outputs  $\mathcal{A}_2(h, h(y))$ . We analysis the probability that  $\mathcal{B}$  inverts  $f_n$  in the following.

$$\begin{aligned} & \Pr[\mathcal{B}(f_n(U_n)) \in f_n^{-1}(f_n(U_n))] \\ & = \mathbf{E}_{h \leftarrow H^{(1)}} [\Pr[\mathcal{A}_2(h, h(f_n(U_n))) \in f_n^{-1}(f_n(U_n))]] \\ & = \mathbf{E}_{h \leftarrow H^{(1)}} \left[ \sum_{x \in \{0,1\}^n} \Pr[f_n(U_n) = f_n(x) \wedge \mathcal{A}_2(h, h(f_n(x))) = x] \right] \\ & = \mathbf{E}_{h \leftarrow H^{(1)}} \left[ \sum_{\eta, x \text{ s.t. } \eta = h(f_n(x))} \Pr[f_n(U_n) = f_n(x)] \cdot \Pr[\mathcal{A}_2(h, \eta) = x] \right] \\ & \geq \mathbf{E}_{h \leftarrow H^{(1)}} \left[ \sum_{\eta, x \text{ s.t. } x \in W_{h,\eta}} \Pr[f_n(U_n) = f_n(x)] \cdot \Pr[\mathcal{A}_2(h, \eta) = x] \right] \\ & \geq 2^{-t-\Delta_3} \cdot \mathbf{E}_{h \leftarrow H^{(1)}} \left[ \sum_{\eta, x \text{ s.t. } x \in W_{h,\eta}} \Pr[\mathcal{A}_2(h, \eta) = x] \right] \\ & = 2^{-t-\Delta_3} \cdot 2^{t-\Delta_1} \cdot \Pr[\mathcal{A}_2(H^{(1)}, U_{t-\Delta_1}) \in W_{H^{(1)}, U_{t-\Delta_1}}] \\ & \geq 2^{-(\Delta_1+\Delta_3)} \cdot \frac{\varepsilon(n)^4}{64} \\ & = s(n)^{-3/4} \cdot \frac{\varepsilon(n)^4}{64}, \end{aligned}$$

which is greater than  $1/s(n)$  if  $\varepsilon$  is non-negligible.

Next, we consider the case  $x \notin S_t$ . We define  $W_y = \{(h, h(x)) : h \in H^{(2)} \text{ and } x \in f_n^{-1}(y)\} \subseteq \{0, 1\}^q$ , where  $q$  is the length of  $(h, h(x))$ . Any (possibly cheating) quantum state

$|\psi\rangle$  for the second commitment can be written as follows:

$$|\psi\rangle = \sum_{z \in W_y} \alpha_z |z\rangle_+ + \sum_{z \notin W_y} \alpha_z |z\rangle_+,$$

since  $\{|z\rangle_+\}_{z \in \{0,1\}^q}$  is a basis. Then  $b_0(n) = \sum_{z \in W_y} |\alpha_z|^2$ . Since  $|\psi\rangle$  can be written as

$$|\psi\rangle = \sum_{u \in W_y} \sum_{z \in \{0,1\}^q} \alpha_z (-1)^{\langle u, z \rangle} |u\rangle_\times + \sum_{u \notin W_y} \sum_{z \in \{0,1\}^q} \alpha_z (-1)^{\langle u, z \rangle} |u\rangle_\times,$$

$$b_1(n) = \frac{\sum_{u \in W_y} \left| \sum_{z \in \{0,1\}^q} \alpha_z (-1)^{\langle u, z \rangle} \right|^2}{2^q}.$$

To maximize  $b_0(n) + b_1(n)$ , we set  $a = \sum_{z \in W_y} |\alpha_z|^2 = b_0(n)$ . On the condition that  $b_0(n) = a$ ,  $b_1(n)$  achieves the maximum when  $|\alpha_z|$  is uniformly distributed. Actually, it is sufficient to consider the case where

$$\alpha_z = \begin{cases} \sqrt{a/|W_y|} & \text{if } z \in W_y \\ \sqrt{(1-a)/(2^q - |W_y|)} & \text{otherwise.} \end{cases}$$

Then, we have  $b_1(n) = (\sqrt{a|W_y|} + \sqrt{(1-a)(2^q - |W_y|)})^2 / 2^q$ . Let  $\xi = |W_y|/2^q$ . Thus, we have

$$b(n) = 1 + (2a - 1)\xi + 2\sqrt{a(1-a)\xi(1-\xi)}.$$

After some calculation, we have  $b(n) \leq 1 + \sqrt{\xi}$ . Since

$$\xi \leq \frac{|\{x : f_n^{-1}(y)\}|}{2^{n-t-\Delta_2}} \leq \frac{2^{n-t-\Delta_3}}{2^{n-t-\Delta_2}} = 2^{\Delta_2-\Delta_3} = \frac{1}{\sqrt[4]{s(n)}} = \frac{1}{n^{\omega(1)}},$$

we can say that  $b(n) \leq 1 + 1/n^{\omega(1)}$ . □

**Theorem 5.2** *Let  $f = \{f_n : \{0,1\}^n \rightarrow \{0,1\}^n\}_{n \in \mathbb{N}}$  be an  $s(n)$ -secure quantum one-way function family, where  $s(n) = n^{\omega(1)}$ . Then, there exists  $t = t_0 \in [1, n]$  such that Protocol 1 satisfies  $(1/n)$ -hiding if we set  $\Delta_1 = \Delta_2 = \frac{1}{4} \log s(n)$ .*

First, we suppose that  $f$  is a regular quantum one-way function. Then the preimage-size is always constant. This means that  $\mathbf{H}_2(f(U_n))$  is also constant. If the parameter  $t$  is correctly given (i.e.,  $t = \mathbf{H}_2(f(U_n))$ ), the first and the second commitment states are almost maximally mixed. Though there is a small amount of correlation between the first and the second commitment states, we can regard the joint state as a quantum state close to the maximally mixed state by the following lemma, which is a quantum version of Lemma 2.5 in [9].



**Lemma 5.1** *Let  $\rho$  be a mixed state such that  $\rho = \sum_x p_x |x\rangle\langle x| \otimes \rho_x$ . If there exists a mixed state  $\sigma'$  such that  $\delta(\rho_x, \sigma') \leq \varepsilon$  for all  $x$ , then  $\delta(\rho, \sigma) \leq \varepsilon$ , where  $\sigma = \sum_x p_x |x\rangle\langle x| \otimes \sigma'$ .*

**Proof.**

$$\delta(\rho, \sigma) = \frac{1}{2} \text{tr} \sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)} = \frac{1}{2} \sum_x p_x \text{tr} \sqrt{(\rho_x - \sigma')^\dagger (\rho_x - \sigma')} \leq \varepsilon \sum_x p_x = \varepsilon.$$

□

**Proof.** (Theorem ??) We will see the first property. Let  $p(y) = \Pr[f_n(U_n) = y]$  and  $\mu(X) = |X|/2^n$ . For any  $t \in [1, n]$ , let  $A_t = \{y \in \{0, 1\}^n : 2^{-t} \leq p(y) < 2^{-t+1}\}$ . Since  $\bigcup_t A_t = f_n(\{0, 1\}^n)$ , there exists  $t_0$  such that  $\Pr[f_n(U_n) \in A_{t_0}] \geq 1/n$ . Then, we define  $\Gamma_1$  and  $\Gamma_2$  as follows:

$$\begin{aligned} \Gamma_1 &= \{x \in \{0, 1\}^n : p(f_n(x)) < 2^{-t_0+1}\} \text{ and} \\ \Gamma_2 &= \{x \in \{0, 1\}^n : p(f_n(x)) \geq 2^{-t_0}\}, \end{aligned}$$

and set  $\Gamma = \Gamma_1 \cap \Gamma_2$ . Thus, it is easy to see that  $\Gamma_1 \cup \Gamma_2 = \{0, 1\}^n$  and  $\mu(\Gamma) \geq 1/n$ .

Next, we will see the second property. Let  $C_1$  and  $C_2$  be subsystems for  $H_{\text{commit}_1}$  and  $H_{\text{commit}_2}$ , respectively. Assume that Alice has two bits  $w_1$  (resp.,  $w_2$ ) for the first (resp., the second) half of the commitment. Also assume that  $x$  falls into  $\Gamma$ .

Let  $\rho$  be the quantum state  $\text{tr}_{C_2}(\rho_B)$ . Then,  $\rho$  can be written as

$$\rho = \sum_{x \in \Gamma, h \in H^{(1)}} \frac{1}{|\Gamma| \cdot |H^{(1)}|} |h, h(f_n(x))\rangle_{\theta(w_1)} \langle h, h(f_n(x))|.$$

Let

$$\begin{aligned} \iota_+ &= \sum_{z \in \{0, 1\}^{t-\Delta_1}, h \in H^{(1)}} \frac{1}{2^{t-\Delta_1} |H^{(1)}|} |h, z\rangle_+ \langle h, z| \quad \text{and} \\ \iota_\times &= \sum_{z \in \{0, 1\}^{t-\Delta_1}, h \in H^{(1)}} \frac{1}{2^{t-\Delta_1} |H^{(1)}|} |h, z\rangle_\times \langle h, z|. \end{aligned}$$

Then  $\iota \stackrel{\text{def}}{=} \iota_+ = \iota_\times$  is the uniform distribution. By Leftover Hash Lemma, we have  $\delta(\rho, \iota) \leq 2^{-\Delta_1/2}$ .

Next we let  $\rho'(y)$  be the quantum state  $\text{tr}_{C_1}(\rho_B)$  when  $y = f_n(x)$  is given. (Note that any elements in  $f_n^{-1}(y)$  are also in  $\Gamma$ . Thus, the likelihood of  $x$  is the same as that of any other  $x' \in f_n^{-1}(y)$ .) Then,  $\rho'(y)$  can be written as

$$\rho'(y) = \sum_{x \in f_n^{-1}(y), h \in H^{(2)}} \frac{1}{|f_n^{-1}(y)| \cdot |H^{(2)}|} |h, h(x)\rangle_{\theta(w_2)} \langle h, h(x)|.$$

Let

$$\begin{aligned}\iota'_+ &= \sum_{z \in \{0,1\}^{n-t-\Delta_2}, h \in H^{(2)}} \frac{1}{2^{n-t-\Delta_2} |H^{(2)}|} |h, z\rangle_+ \langle h, z| \quad \text{and} \\ \iota'_\times &= \sum_{z \in \{0,1\}^{n-t-\Delta_2}, h \in H^{(2)}} \frac{1}{2^{n-t-\Delta_2} |H^{(2)}|} |h, z\rangle_\times \langle h, z|.\end{aligned}$$

Then  $\iota' \stackrel{\text{def}}{=} \iota'_+ = \iota'_\times$  is the uniform distribution. By Leftover Hash Lemma, we have  $\delta(\rho'(y), \iota') \leq 2^{-\Delta_2/2}$  for any  $y$ . By Lemma 5.1 and the triangle inequality, we have

$$\delta(\rho_B(w_1, w_2), (\iota, \iota')) \leq 2^{-\Delta_1/2} + 2^{-\Delta_2/2} = \frac{2}{\sqrt[8]{s(n)}} = \frac{1}{n^{\omega(1)}}$$

for any  $w_1, w_2 \in \{0, 1\}$ . □

## 6 Hiding Amplification

In the previous section, we showed that Protocol 1 based on quantum one-way function holds a “weak” hiding property. In this section, we amplify the “weak” hiding property to a “strong” one. We consider  $n^2$  parallel executions of Protocol 1 to amplify the hiding probability from  $1/n$  to  $1 - 2^{-n^{\Omega(1)}}$ . We describe the resulting parallel protocol (called Protocol 2) in Figure 3.

In the rest of this section, we state that Protocol 2 achieves  $(1 - 2^{-n^{\Omega(1)}})$ -hiding and preserves the binding property.

**Theorem 6.1** *Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be an  $s(n)$ -secure quantum one-way function family, where  $s(n) = n^{\omega(1)}$ . Then, there exists  $t = t_0 \in [1, n]$  such that Protocol 2 satisfies  $(1 - 2^{-n^{\Omega(1)}})$ -hiding if we set  $\Delta_1 = \Delta_2 = \frac{1}{4} \log s(n)$ .*

Due to the parallel composition, the proof becomes quite simpler than the proof of the hiding amplification in [13]. The proof of Theorem 6.1 can be done by a standard probabilistic argument.

**Proof.** We will see the first property. Recall that  $\Gamma = \{x \in \{0, 1\}^n : 2^{-t_0} \leq p(f_n(x)) < 2^{-t_0+1}\}$  for some  $t_0$ . Let  $N = n^3$  and  $\Gamma' = \{(x_1, \dots, x_{n^2}) \in (\{0, 1\}^n)^{n^2} : \exists i, x_i \in \Gamma\}$ . We consider the probability  $p$  where some  $x_i$  falls in  $\Gamma$ . Since  $\mu(\Gamma) \geq 1/n$ , we have that  $p > 1 - (1 - 1/n)^{n^2}$ . By the fact that  $1 - t < e^{-t}$ , we have  $p \geq 1 - e^{-n} > 1 - 2^{-n} = 1 - 2^{-N^{1/3}}$ .

Next, we will see the second property. Let  $(x_1, \dots, x_{n^2}) \in \Gamma'$ . By the definition of  $\Gamma'$ , we may assume that  $x_J \in \Gamma$  for some  $J \in [1, n^2]$ . Recall that  $Z_1(w_1)$  is of the form

$$|h_{1,1}, h_{1,1}(f_n(x_1))\rangle_{\theta(w_{1,1})} \otimes \cdots \otimes |h_{1,n^2}, h_{1,n^2}(f_n(x_{n^2}))\rangle_{\theta(w_{1,n^2})}$$

---

**Parameters:** Integers  $t \in [1, n]$ ,  $\Delta_1 \in [0, t]$  and  $\Delta_2 \in [0, n - t]$ .

**Commit Phase:**

1. Alice with her two bits  $w_1$  and  $w_2$  first chooses  $x_1, \dots, x_{n^2} \in (\{0, 1\}^n)^{n^2}$  uniformly and computes  $y_1 = f_n(x_1), \dots, y_{n^2} = f_n(x_{n^2})$ . Also, she uniformly and independently chooses pairwise independent hash functions  $h_{1,1}, \dots, h_{1,n^2} \in (H^{(1)})^{n^2}$  and  $h_{2,1}, \dots, h_{2,n^2} \in (H^{(2)})^{n^2}$ .
2. Alice chooses  $w_{1,1}, \dots, w_{1,n^2} \in (\{0, 1\})^{n^2}$  and  $w_{2,1}, \dots, w_{2,n^2} \in (\{0, 1\})^{n^2}$  such that  $w_1 = w_{1,1} \oplus \dots \oplus w_{1,n^2}$  and  $w_2 = w_{2,1} \oplus \dots \oplus w_{2,n^2}$ .
3. Next, Alice sends the quantum state

$$\begin{aligned} & |h_{1,1}, h_{1,1}(y_1)\rangle_{\theta(w_{1,1})} \otimes \dots \otimes |h_{1,n^2}, h_{1,n^2}(y_{n^2})\rangle_{\theta(w_{1,n^2})} \\ & \otimes |h_{2,1}, h_{2,1}(x_1)\rangle_{\theta(w_{2,1})} \otimes \dots \otimes |h_{2,n^2}, h_{2,n^2}(x_{n^2})\rangle_{\theta(w_{2,n^2})} \in (\mathbf{H}_{\text{commit}_1})^{\otimes n^2} \otimes (\mathbf{H}_{\text{commit}_2})^{\otimes n^2} \end{aligned}$$

to Bob.

4. Bob then stores the received quantum state  $\rho_B$  until the reveal phase.

**Reveal Phase:**

1. Alice announces the first decommitments  $(w_{1,1}, h_{1,1}, y_1), \dots, (w_{1,n^2}, h_{1,n^2}, y_{n^2})$  and the second decommitments  $(w_{2,1}, h_{2,1}, x_1), \dots, (w_{2,n^2}, h_{2,n^2}, x_{n^2})$  to Bob.
2. Next, Bob measures the first register of  $\rho_B$  with measurement

$$\{P_{\theta(w_{1,1})}^{h,z}\}_{h \in H^{(1)}, z \in \text{range}(h_{1,1})} \otimes \dots \otimes \{P_{\theta(w_{1,n^2})}^{h,z}\}_{h \in H^{(1)}, z \in \text{range}(h_{1,n^2})}$$

and obtains the classical output  $(h_1, z_1, \dots, h_{n^2}, z_{n^2})$ , where each  $(h_i, z_i)$  is in  $H^{(1)} \times \text{range}(h_{1,i})$ . Also he simultaneously measures the second register with measurement

$$\{P_{\theta(w_{2,1})}^{h',z'}\}_{h' \in H^{(2)}, z' \in \text{range}(h_{2,1})} \otimes \dots \otimes \{P_{\theta(w_{2,n^2})}^{h',z'}\}_{h' \in H^{(2)}, z' \in \text{range}(h_{2,n^2})}$$

and obtains the classical output  $(h'_1, z'_1, \dots, h'_{n^2}, z'_{n^2})$ , where each  $(h'_i, z'_i)$  is in  $H^{(2)} \times \text{range}(h_{2,i})$ .

3. Lastly, Bob accepts the first commitment if and only if  $h_i(y_i) = z_i$  for every  $i$ , and recovers the first committed bit  $w_1$  as  $w_1 = w_{1,1} \oplus \dots \oplus w_{1,n^2}$ . Also he accepts the second commitment if and only if  $h'_i(z'_i) = x_i$  and  $y_i = f_n(x_i)$  for every  $i$ , and recovers the second committed bit  $w_2$  as  $w_2 = w_{2,1} \oplus \dots \oplus w_{2,n^2}$ .
- 

Figure 3: Protocol 2

and  $Z_2(w_2)$  is of the form

$$|h_{2,1}, h_{2,1}(x_1)\rangle_{\theta(w_{2,1})} \otimes \cdots \otimes |h_{2,n^2}, h_{2,n^2}(x_n^2)\rangle_{\theta(w_{2,n^2})}.$$

Let  $W(x_i, w_{1,i}, w_{2,i})$  be the composition of the  $i$ -th components of  $Z_1(w_1)$  and  $Z_2(w_2)$ , that is,

$$W(x_i, w_{1,i}, w_{2,i}) = |h_{1,i}, h_{1,i}(f_n(x_i))\rangle_{\theta(w_{1,i})} |h_{2,i}, h_{2,i}(x_i)\rangle_{\theta(w_{2,i})}.$$

Since  $w_{1,1}, \dots, w_{1,n^2}$  and  $w_{2,1}, \dots, w_{2,n^2}$  are randomly chosen so as to satisfy that  $w_1 = w_{1,1} \oplus \cdots \oplus w_{1,n^2}$  and  $w_2 = w_{2,1} \oplus \cdots \oplus w_{2,n^2}$ , we may assume that  $w_{1,j}$  and  $w_{2,j}$  with  $j \neq J$  are uniformly and independently chosen from  $\{0, 1\}$  and  $w_{1,J}$  and  $w_{2,J}$  are determined by  $w_1$ ,  $w_2$ , and all  $w_{1,j}$  and  $w_{2,j}$  such that  $j \neq J$ . Thus, we can say that  $W(x_i, w_{1,i}, w_{2,i})$  such that  $i \neq J$  does not depend on the value of  $w_1$  and  $w_2$ .

On the other hand,  $W(x_J, w_{1,J}, w_{2,J})$  depends on the value  $w_1$  and  $w_2$ . But, we can show that it is  $1/n^{\omega(1)}$ -close to the uniform distribution by using the proof for the 2nd property of Theorem 5.2. From Lemma 5.1, we can say that  $(Z_1(0), Z_2(0))$ ,  $(Z_1(0), Z_2(1))$ ,  $(Z_1(1), Z_2(0))$  and  $(Z_1(1), Z_2(1))$  are  $1/n^{\omega(1)}$ -close to each other.  $\square$

**Theorem 6.2** *Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be an  $s(n)$ -secure quantum one-way function family, where  $s(n) = n^{\omega(1)}$ . Then Protocol 2 with setting of parameters  $\Delta_1 = \Delta_2 = \frac{1}{4} \log s(n)$ , is a 2-parallel quantum bit commitment scheme that is computationally 1-out-of-2 binding regardless of the setting of  $t$ .*

The above theorem says that Protocol 2 has 1-out-of-2 binding property. Specifically speaking, the computational binding of the first half commitment can be guaranteed in some case and the statistical binding of the second half commitment can be guaranteed in the other case. The computational binding of the first half commitment in Protocol 2 is reduced to the computational binding of the first half commitment in Protocol 1. The statistical binding of the second half commitment in Protocol 2 can be shown by a probabilistic argument.

To prove that Protocol 2 is computationally 1-out-of-2 binding, we have to specify a set that controls the 1-out-of-2 property as in the proof of Theorem 5.1. In the proof of Theorem 5.1,  $S_t$  is such a set. For the proof of Theorem 6.2, we will use  $S'_t = \{(x_1, \dots, x_{n^2}) \in (\{0, 1\}^n)^{n^2} : \exists i, x_i \in S_t\}$ . Even if we can use the reduction to the  $j$ -th subprotocol, we cannot know whether  $x_j \in S_t$  or not. If  $x_j \in S_t$ , then the reduction goes through. If we cannot assume that  $x_j \in S_t$ , we can say that  $x_j \in \{0, 1\}^n$ . Since we do not have to know some underlying relation to apply Non-interactive Quantum Hashing Theorem, we can show that the reduction still goes through.

**Proof.** The proof is similar to the proof for Theorem 5.1. For every  $t \in [1, n]$ , we define the set of “heavy” strings to be

$$S'_t = \{(x_1, \dots, x_{n^2}) \in (\{0, 1\}^n)^{n^2} : \exists i, x_i \in S_t\},$$

where  $S_t$  is defined in the proof of Theorem 5.1.

We will show that if  $(x_1, \dots, x_{n^2}) \in S'_t$  is chosen in the first step of Commit Phase then the first half is binding and if  $(x_1, \dots, x_{n^2}) \notin S'_t$  then the second half is binding.

First, we show a reduction from inverting  $f_n$  to violating the binding property of Protocol 2 in the case of  $(x_1, \dots, x_{n^2}) \in S'_t$ . Recall that in the proof of Theorem 5.1  $f'_n : H^{(1)} \times \{0, 1\}^n \rightarrow H^{(1)} \times \{0, 1\}^{t-\Delta_1}$  is a function that maps  $(h, x)$  to  $(h, h(f_n(x)))$ ,  $R'_n = \{(f'_n(h, x), (h, x)) : x \in S_t \text{ and } h \in H^{(1)}\}$  and  $W_{h, \eta} = \{x \in \{0, 1\}^n : (\eta, (h, x)) \in R'_n\}$ . We also define  $R_n = \{(f'_n(h, x), (h, x)) : x \in \{0, 1\}^n \text{ and } h \in H^{(1)}\}$ .

Let  $\mathcal{A}_3$  be a quantum algorithm to violate the binding property of Protocol 2 with probability  $\varepsilon(n)$ . This means that  $\mathcal{A}_3$  can send a quantum state in Commit Phase so that Bob can accept it either as 0-commitment with probability  $b_0(n)$  and as 1-commitment with probability  $b_1(n)$ , where  $b(n) = b_0(n) + b_1(n) \geq 1 + \varepsilon(n)$ . To make Bob accept the quantum state as a valid commitment in Protocol 2,  $\mathcal{A}_3$  has to make Bob accept all executions of sub-protocol Protocol 1. Let  $b_w^{(i)}(n)$  be the probability that  $\mathcal{A}_3$  can make Bob accept the  $i$ -th sub-protocol as  $w$ -commitment. We set  $b^{(i)}(n) = b_0^{(i)}(n) + b_1^{(i)}(n)$ . Let  $\tilde{b}_0(n)$  (resp.,  $\tilde{b}_1(n)$ ) be the probability where  $\mathcal{A}_3$  fails to make Bob accept the quantum state as 0-commitment (resp., 1-commitment). Similarly, we define  $\tilde{b}_0^{(i)}(n)$  and  $\tilde{b}_1^{(i)}(n)$  for each  $i \in [1, n^2]$ . Then, we have  $\tilde{b}_0(n) + \tilde{b}_1(n) \leq 1 - \varepsilon$ . Since the failure probabilities are accumulative, there exists an index  $j \in [1, n^2]$  such that  $\tilde{b}_0^{(j)}(n) + \tilde{b}_1^{(j)}(n) \leq 1 - \varepsilon$ . Hence, we have  $b_0^{(j)}(n) + b_1^{(j)}(n) \geq 1 + \varepsilon$ . Thus, we can assume that a quantum algorithm  $\mathcal{A}_4$  to violate the binding property of Protocol 1 with probability  $\varepsilon$ . Note that the violation (by  $\mathcal{A}_4$ ) against the binding property of Protocol 1 is respect to either  $R_n$  or  $R'_n$ . Fortunately, we do not have to know which relation should be considered, since the algorithm with respect to  $R_n$  is the same as the one with respect to  $R'_n$ . If  $\mathcal{A}_4$  violates the binding property of the  $j$ -th sub-protocol and  $x_j \in S_t$ ,  $\mathcal{A}_4$  does with respect to  $R'_n$ . If  $\mathcal{A}_4$  violates the binding property of the  $j$ -th sub-protocol and  $x_j \in \{0, 1\}^n$ ,  $\mathcal{A}_4$  does with respect to  $R_n$ . Here, we consider only the case that  $\mathcal{A}_4$  does with respect to  $R'_n$ , since the other case is similar and easier to show.

From Theorem 4.1, we have another algorithm  $\mathcal{A}_5$  satisfying that

$$\begin{aligned} \Pr[\mathcal{A}_5(H^{(1,1)}, H^{(1,1)}(f_n(U_n^{(1)})), \dots, H^{(1,n^2)}, H^{(1,n^2)}(f_n(U_n^{(n^2)}))) = (j, z) \\ \wedge z \in W_{H^{(1,j)}, H^{(1,j)}(f_n(U_n^{(j)}))}] \geq \varepsilon(n)^2/4, \end{aligned}$$

where  $H^{(1,1)}, \dots, H^{(1,n^2)}$  are independent and identical distributions to  $H^{(1)}$  and  $U_n^{(1)}, \dots, U_n^{(n^2)}$  are independent and identical distributions to  $U_n$ .

By the similar discussion in the proof of Theorem 5.1, we can say that

$$\begin{aligned} \Pr[\mathcal{A}_5(H^{(1,1)}, H^{(1,1)}(f_n(U_n^{(1)})), \dots, H^{(1,j-1)}, H^{(1,j-1)}(f_n(U_n^{(j-1)})), H^{(1,j)}, U_{t-\Delta}, \\ H^{(1,j+1)}, H^{(1,j+1)}(f_n(U_n^{(j+1)})), \dots, H^{(1,n^2)}, H^{(1,n^2)}(f_n(U_n^{(n^2)}))) = (j, z) \\ \wedge z \in W_{H^{(1,j)}, U_{t-\Delta_1}}] \geq \varepsilon(n)^4/64. \end{aligned}$$

We consider an algorithm  $\mathcal{B}$  that on input  $y = f_n(x)$ , picks randomly an integer  $j' \in [1, n^2]$ , a hash function  $h \in H^{(1)}$ .  $\mathcal{B}$  also picks randomly  $x_1, \dots, x_{j'-1}, x_{j'+1}, \dots, x_{n^2}$  and

$h_1, \dots, h_{j'-1}, h_{j'+1}, \dots, h_{n^2}$ , computes  $y_1 = f_n(x_1), \dots, y_{j'-1} = f_n(x_{j'-1}), y_{j'+1} = f_n(x_{j'+1}), \dots, y_{n^2} = f_n(x_{n^2})$  and outputs the second part of  $\mathcal{A}_5(h_1, h_1(y_1), \dots, h_{j'-1}, h_{j'-1}(y_{j'-1}), h, h(y), h_{j'+1}, h_{j'+1}(y_{j'+1}), \dots, h_{n^2}, h_{n^2}(y_{n^2}))$ . Then, we have the following.

$$\begin{aligned}
& \Pr[\mathcal{B}(f_n(U_n)) \in f_n^{-1}(f_n(U_n))] \\
& \geq \mathbf{E}_{h \leftarrow H^{(1)}} [\Pr[\mathcal{A}_5(h_1, h_1(f_n(U_n^{(1)})), \dots, h_{j'-1}, h_{j'-1}(f_n(U_n^{(j'-1)})), h, h(f_n(U_n)), \\
& \quad h_{j'+1}, h_{j'+1}(f_n(U_n^{(j'+1)})), \dots, h_{n^2}, h_{n^2}(f_n(U_n^{(n^2)}))) = (j, z) \\
& \quad \wedge j = j' \wedge z \in f_n^{-1}(f_n(U_n))]] \\
& = \frac{1}{n^2} \cdot \mathbf{E}_{h \leftarrow H^{(1)}} [\Pr[\mathcal{A}_5(h_1, h_1(f_n(U_n^{(1)})), \dots, h_{j'-1}, h_{j'-1}(f_n(U_n^{(j'-1)})), h, h(f_n(U_n)), \\
& \quad h_{j'+1}, h_{j'+1}(f_n(U_n^{(j'+1)})), \dots, h_{n^2}, h_{n^2}(f_n(U_n^{(n^2)}))) = (j, z) \\
& \quad \wedge z \in f_n^{-1}(f_n(U_n))]].
\end{aligned}$$

The rest of the probabilistic analysis is similar to the proof of Theorem 5.1. This shows that

$$\Pr[\mathcal{B}(f_n(U_n)) \in f_n^{-1}(f_n(U_n))] \geq s(n)^{-3/4} \cdot \varepsilon(n)^4 / 64n^2,$$

which is greater than  $1/s(n)$  if  $\varepsilon$  is non-negligible.

Next, we consider the case  $(x_1, \dots, x_{n^2}) \notin S'_t$ . By the definition of  $S'_t$ , we have  $x_i \notin S_t$  for all  $i$ . Thus, we can use the discussion for the proof of Theorem 5.1 for each bit  $w_{2,i}$ . This means that the value of  $b^{(i)}(n)$  is less than  $1 + 1/n^{\omega(1)}$  for each bit  $w_{2,i}$ . Let us consider the event that Bob accepts the quantum state sent by Alice in Commit Phase of Protocol 2 as 0-commitment (or, 1-commitment). Let  $p$  be the probability that this event occurs. Since this even occurs if Bob accepts all decommitments of the sub-protocol, we can write  $p = p_1 \cdots p_{n^2}$ , where  $p_i$  is either the probability that Bob accepts the quantum state sent by Alice in Commit Phase of the  $i$ -th sub-protocol as 0-commitment or the probability that Bob accepts the quantum state sent by Alice in Commit Phase of the  $i$ -th sub-protocol as 1-commitment. Thus, the best strategy for cheating is to behave honestly for  $n^2 - 1$  executions of the sub-protocol and maliciously for just one execution. Hence, we can upper-bound  $b(n)$  by  $1^{n^2-1}(1 + 1/n^{\omega(1)}) = 1 + 1/n^{\omega(1)}$ .  $\square$

## 7 Statistically-Hiding Commitment from $\binom{2}{1}$ -Binding Commitment

We have obtained the strongly-hiding 1-out-of-2 binding quantum commitment based on quantum one-way function. But it is not a single scheme but a family of scheme candidates. First, we construct a family of candidates for normal statistically-hiding quantum bit commitment from the family of candidates for the strongly-hiding 1-out-of-2 binding quantum commitment. Next, we construct a single normal statistically-hiding quantum bit commitment from the family of candidates for the statistically-hiding quantum bit commitment.

## 7.1 Statistically-Hiding Quantum Commitment Family from $\binom{2}{1}$ -Binding Quantum Commitment Family

Protocol 2 consists of the first half commitment and the second half commitment. We denote by  $\text{P2first}(w_1)$  the first half commitment with the committed bit  $w_1$  and by  $\text{P2second}(w_2)$  the second half commitment with the committed bit  $w_2$ . We consider the protocol (called Protocol 3) in Figure 4.

---

**Parameters:** Integers  $t \in [1, n]$ ,  $\Delta_1 \in [0, t]$  and  $\Delta_2 \in [0, n - t]$ . (These are succeeded to the sub-protocol  $\text{P2first}$  and  $\text{P2second}$ .)

**Commit Phase:**

1. Alice with her bit  $w$  executes  $\text{P2first}(w)$  and  $\text{P2second}(w)$  in parallel.

**Reveal Phase:**

1. Alice sends decommitments for  $\text{P2first}(w)$  and  $\text{P2second}(w)$  and Bob recovers the committed bits  $w'$  and  $w''$ , respectively.
  2. Bob verifies the correctness of the decommitments. If the verification procedures for both  $\text{P2first}(w)$  and  $\text{P2second}(w)$  are passed and  $w' = w''$  then Bob accepts.
- 

Figure 4: Protocol 3

**Theorem 7.1** *Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be an  $s(n)$ -secure quantum one-way function family, where  $s(n) = n^{\omega(1)}$ . Then Protocol 3 with setting of parameters  $\Delta_1 = \Delta_2 = \frac{1}{4} \log s(n)$ , is a computationally-binding quantum bit commitment scheme regardless of the setting of  $t$ . Also, there exists  $t = t_0 \in [1, n]$  such that Protocol 3 with the same parameter for  $\Delta_1$  and  $\Delta_2$  is statistically-hiding.*

The hiding property can be shown by the argument in the proof of Theorem 6.1. Basically, Protocol 3 has the 1-out-of-2 binding property. Thus, either  $\text{P2first}$  or  $\text{P2second}$  must have the binding property. Even if the adversary can violate either  $\text{P2first}$  or  $\text{P2second}$ , such violation can be detected by the equality check  $w' = w''$  in Reveal Phase. Theorem 7.1 can be similarly shown as Theorems 6.1 and 6.2.

## 7.2 From a family To single BC

As mentioned in Theorem 7.1, there exists a value  $t$  such that Protocol 3 has both the computational binding and statistical hiding. But, we do not know the right value of  $t$ . By using a similar technique in Section 7, we consider a combined protocol of Protocol with different parameters.

$P3(t, w)$  denotes the commit phase of Protocol 3 with the committed value  $w$  and parameter  $t$ . We consider the protocol (called Protocol 4) in Figure 5.

---

**Parameters:** Integers  $\Delta_1 \in [0, t]$  and  $\Delta_2 \in [0, n - t]$ . (These are succeeded to the sub-protocol P3.)

**Commit Phase:**

1. Alice with her bit  $w$  chooses  $w_1, \dots, w_n \in (\{0, 1\})^n$  such that  $w = w_1 \oplus \dots \oplus w_n$ .
2. Alice executes  $P3(1, w_1), \dots, P3(n, w_n)$  in parallel.

**Reveal Phase:**

1. Alice sends decommitment of  $P3(i, w_i)$  for each  $i$  and Bob obtains the committed bits  $w'_i$  for all  $i$  and computes  $w' = w'_1 \oplus \dots \oplus w'_n$ .
  2. Bob verifies the correctness of the decommitments. If all the verification procedures are passed then Bob accepts.
- 

Figure 5: Protocol 4

**Theorem 7.2** *Let  $f = \{f_n : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{n \in \mathbb{N}}$  be an  $s(n)$ -secure quantum one-way function family, where  $s(n) = n^{\omega(1)}$ . Then Protocol 4 with setting of parameters  $\Delta_1 = \Delta_2 = \frac{1}{4} \log s(n)$ , is a computationally-binding and statistically-hiding quantum bit commitment scheme.*

Theorem 7.2 can be also shown as Theorems 6.1 and 6.2.

## 8 Concluding Remarks

We have derived a quantum and non-interactive version (Non-interactive Quantum Hashing Theorem) of the new interactive hashing theorem. As its application, we have constructed a statistically-hiding non-interactive quantum bit commitment scheme. We note that by using the same discussion we can show the parallel composability of our quantum bit commitment scheme.

In classical cryptography, the interactive hashing theorem has many applications. So, we hope that Non-interactive Quantum Hashing Theorem also has many applications to quantum cryptography.

## Acknowledgments

A part of the research was done while the first author was at Université Paris-Sud 11 and supported by JST-CNRS project on “Quantum Computation: Theory and Feasibility” and



the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (B), 21300002, 2010 and for Exploratory Research, 20650001, 2010.

## References

- [1] D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C.-C. Yao: Quantum bit escrow, in *Proc. 32nd ACM Symp. Theory of Computing*, pp.705–714 (2000).
- [2] C. H. Bennett and G. Brassard: Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conf. Computers, Systems, and Signal Processing, Bangalore, India*, pp.175–179. IEEE, New York (1984).
- [3] G. Brassard, D. Chaum, and C. Crépeau: Minimum disclosure proofs of knowledge, *J. Comput. Syst. Sci.* 37(2):156–189 (1988).
- [4] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner: Possibility, impossibility and cheat-sensitivity of quantum bit string commitment, *Phys. Rev. A* 78(32), 022316 (2008).
- [5] J. L. Carter and M. N. Wegman: Universal classes of hash functions, *J. Comp. Syst. Sci.* 18(2):143–154 (1979).
- [6] C. Crépeau, P. Dumais, D. Mayers, and L. Salvail: Computational collapse of quantum state with application to oblivious transfer, in *Proc. 1st Theory of Cryptography Conference*, Lect. Notes Comput. Sci. 2951, pp.374–393 (2004).
- [7] I. Damgård, S. Fehr, R. Renner, L. Salvail, C. Schaffner: A tight high-order entropic quantum uncertainty relation with applications, in *Advances in Cryptology — CRYPTO 2007*, Lect. Notes Comput. Sci. 4622, pp.360–378 (2007).
- [8] P. Dumais, D. Mayers, and L. Salvail: Perfectly concealing quantum bit commitment from any quantum one-way permutation, in *Advances in Cryptology — EUROCRYPT 2000*, Lect. Notes Comput. Sci. 1807, pp.300–315 (2000).
- [9] A. Gabizon, R. Raz, and R. Shaltiel: Deterministic extractors for bit-fixing sources by obtaining an independent seed. *SIAM J. Comput.* 36(4):1072–1094 (2006).
- [10] O. Goldreich, S. Micali, and A. Wigderson: Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems, *J. ACM* 38(3):691–729 (1991).
- [11] I. Haitner, J. J. Hoch, O. Reingold, and G. Segev: Finding collisions in interactive protocols — A tight lower bound on the round complexity of statistically-hiding commitments, in *Proc. 48th IEEE Symp. Foundations of Computer Sciences*, pp.669–679 (2007).

- [12] I. Haitner, O. Horvitz, J. Katz, C.-Y. Koo, R. Morselli, and R. Shaltiel: Reducing complexity assumptions for statistically-hiding commitment, *J. Cryptol.* 22(3):283–310 (2009).
- [13] I. Haitner, M. Nguyen, S.J. Ong, O. Reingold, and S.P. Vadhan: Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM J. Comput.* 39(3):1153–1218 (2009).
- [14] I. Haitner and O. Reingold: A new interactive hashing theorem, in *Proc. 22nd IEEE Conf. Computational Complexity*, pp.319–332 (2007).
- [15] I. Haitner and O. Reingold: Statistically-hiding commitment from any one-way function, in *Proc. 39th ACM Symp. Theory of Computing*, pp.1–10 (2007).
- [16] I. Haitner, O. Reingold, S.P. Vadhan, and H. Wee: Inaccessible entropy, in *Proc. 41st ACM Symp. Theory of Computing*, pp.611–620 (2009).
- [17] L. Hardy and A. Kent: Cheat sensitive quantum bit commitment, *Phys. Rev. Lett.* 92(15), 157901 (2004).
- [18] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby: A pseudorandom generator from any one-way function, *SIAM J. Comput.* 28(4):1364–1396 (1999).
- [19] A. Kent: Quantum bit string commitment, *Phys. Rev. Lett.* 90(23), 237901 (2003).
- [20] T. Koshiha and T. Odaïra: Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function, in *Proc. 4th Workshop on Theory of Quantum Computation, Communication, and Cryptography* (TQC 2009), Lect. Notes Comput. Sci. 5906, pp.33–46, 2009.
- [21] H.-K. Lo and H. F. Chau: Is quantum bit commitment really possible?, *Phys. Rev. Lett.* 78(17):3410–3413 (1997).
- [22] D. Mayers: Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.* 78(17):3414–3417 (1997).
- [23] M. Naor: Bit commitment using pseudorandomness, *J. Cryptol.* 4(2):151–158 (1991).
- [24] M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung: Perfect zero-knowledge arguments for NP using any one-way permutation, *J. Cryptol.* 11(2):87–108 (1998).
- [25] M.-H. Nguyen, S.-J. Ong, and S. P. Vadhan: Statistical zero-knowledge arguments for NP from any one-way function, *Proc. 47th IEEE Symp. Foundations of Computer Science*, pp.3–14 (2006).
- [26] P. W. Shor: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* 26(5):1484–1509 (1997).